Some Technologies for Information Security Protection in Weak-controlled Computer Systems and Their Applicability for eGovernment Services Users

Anton Palazov

University of National and World Economy, Department of Information Technologies and Communications, UNSS, 1700 Sofia, Bulgaria
apalazov@rubella.bg

Abstract. The users of eGovernment services start exchanging documents with administrative authorities, making ePayments, and in such communications the risks of confidential information disclosure and direct financial losses are growing up. The computer systems of these users are weak-controlled and are outside of sphere of well-defined information security protection decisions. The technologies for data protection in case of theft or loss of computers and data devices and in case of data leakage are very important for eGovernment services users and must have appropriate properties to be useful for their security needs. A model of anti-theft technology implementation, which disables stolen computers and can send them data-destructive commands to erase sensitive data ,is presented. The technologies for control over the channels which can lead to data leakage protect data by whitelisting or blacklisting some devices or ports, by prohibit and allow some actions and operations, or by transparent encryption of outbound data. Some technologies for control over the leaving data use pre-defined set of sensitive data type definitions. Users can select definitions to apply or can customize some of them according specific conditions or regulations. At the end some conclusions about applicability of anti-theft and sensitive data leakage prevention technologies for protection of information security of eGovernment users was done.

Key words: eGovermnemt services users, anti-theft, data leakage prevention, sensitive data type definitions

1 eGovernment users evolution and risks for their information security

In time, the users of eGovernment services get more experience and possibilities and start performing more complex tasks - exchange of documents with administrative authorities in electronic form which can have legal consequences for both sides, making ePayments for tax duties, receiving money from social funds etc.

In such more complex communucations the risks of confidential information disclosure and direct financial losses are growing up and information security protection system must mitigate them and counteract to the fault. Computer theft, data device losses and leakage of important user data are the events, which can transform these security risks to attacks against user privacy.

The survey of Ponemon institute [11] for endpoint security in 2009 shows that the loss of sensitive data is real event for about 50 percents of analyzed companies (respondents). The results for lost or stolen computing devices are almost the same. The interviewed security professionals give the opinion that these risks will be one of their main troubles in next 12 months. The users of eGovernment services interact with the administrative authorities mainly with their home computers thru the Internet. These computers are outside the protecion of information security based on well-defined from computer professionals, good supported and strongly enforced security policy as is the case of corporate information systems. From point of view of information security protection the computer system of typical eGovernment users are weak-controlled and in many cases there is no implementation of clear and reliable security rules [1], [2].

So, the technologies for data protection in case of theft or loss of computers and data devices and in case of data leakage are very important for eGovernment services users and must have appropriate properties to be useful for their information security protection.

In this research the following steps are performed:

- Study and analysis of publications in magazines and in Internet and defining of criterias for estimating of technologies applicability in information security protection;
- Specifying of main parameters and characteristics of analyzed technologies;
- Measuring and conclusions formulation about analyzed technologies applicability in information security protection of eGovernment services users.

2 Technologies for Client-side protection for lost or stolen computer systems and for stand-alone data leakage prevention

Endpoint computer systems (servers, desktops, laptops) and removable media (CD, DVD, USB memory) are especially vulnerable to security accidents like loss or theft, which makes them a weak spot in information systems infrastructure [10]. Companies and citizens need security solutions that can protect their information systems against these threats and ensure that unauthorized persons have no access to their saved sensitive data.

2.1 Protection of lost or stolen computer systems and data devices

Loss or theft of computer systems, devices or data files is significant risk for information confidentiality. Security protection technologies must react on these

events with registering of stolen systems, disabling them, sending a data-destructive commands to erase sensitive data and easily reactivating them if they are recovered.

The vendors of Endpoint protection platforms [5], [7] offer different solutions for data protection in case of theft or loss of computer systems. The basic characteristics of these solutions can be summarized as:

- Protected user computers have internal timer (software module or hardware device) which try to communicate with Ownership Management Server via Internet. The duration of the interval between two connections can be set from the user or remotely from the server or administrator;
- If the user computer can't connect to the Management server in the defined for the timer interval or communication schedule, the timer suppose that the computer was lost and activates the transparent service which disables user sensitive data and the computer system itself;
- If the computer was lost, its user can call the Ownership Management Center help desk and can register the event. When the lost or stolen computers connect later to the server in their regular communications, the server can send to the workstation self-destructive signal. The internal timer on the lost computer system react to that signal and disables in some ways sensitive user data and probably the computer system itself;
- The Ownership Management Server has possibilities to submit the one-time activation key, which can be used to enable the computer in case it was found and its owner can authenticate himself.

By adding this client-side intelligence the confidentiality of sensitive user data can be reliably protected in case of loss, theft or suspicious circumstances - the internal timer on client computer systems or the signal from the server will automatically disable these data and will not allow the attacker to exploit them.

2.2 Standalone endpoint data leakage prevention

The technologies for endpoint data leakage protection can be divided in 2 general groups:

- First, technologies for control over the channels, which can lead to data leakage (data devices, ports, Internet services), and;
- Second, technologies for control over the data, which leave the computer system in different directions.

Technologies for channel control [8] protects data by whitelisting or blacklisting specific devices or ports, by prohibit and allow some actions and operations in available channels, or by transparent encryption of data that go out of information security protection system. In case of encryption users can apply existing PKI infrastructure or can define their own keys or passwords for removable media, file types or specific files and communication units which will be exchanged with their partners.

Endpoint users need to encrypt some removable media to protect data confidentiality and to allow access to them via some unlock mechanism (passwords, keys for decryption, etc), which is shared with other partners. They can protect the whole media, particular file types, or specific data files. Central management helps security administrators to create, implement, enforce and audit secirity policies for different groups, users or business partners.

Technologies for control over the leaving data offer possibilities for content detection, which, by example, can include SSN or VAT number identification in exchanged documents. Some solutions [9] can detect in outbound flow other specific "registered" data elements such as database field values and aggregates, file names, register keys, etc. These tools use number of dictionaries where are defined, by example, financial items, legal term, trade marks. The dictionaries allow using of "wild card", operators and case-sensitivity indicators. Some of them have intelligence features which do more than just a formal search in data content.

Both groups of technologies provide decisions for data leak prevention by restricting unauthorized export of confidential data via certain communication ports or peripheral devices. Security policies define some read and write restrictions on ports and devices based on device type, data file types or even on individual peripheral devices or files. Additional software components apply and control compliance with defined security rules.

Some vendors [7] offer tools which include valuable set of sensitive data type definitions created by their security professionals. Those tools are integrated with threats detection engines and ensure immediate data leakage prevention after their installation. Pre-defined set of sensitive data type definitions contain ready-for-use rules for PII (Personal Identifiable Information), intellectual property elements and other data types like credit cards, bank accounts, national identification numbers, social security number, etc. Users can either select which data type definitions from this set to apply on their endpoints or customize some of them for their own conditions, regulations or needs.

Flexible security policies wizards allow them also to define objects for content scanning including endpoints and groups, email senders and recipients, file and device types. In these tools events that trigger them can be selected - content copying to a removable storage device, uploading content in browsers and IM clients, sending data via email. In such events DLP can log the event, warn the user, block the transaction, quarantine or encrypt the content before sending.

Some software tools try to analyze and assess former communications from historical archives in protected system and to generate additional security rules from that gather knowledge that, with such learning approach, counteract more reliably to sensitive data leakage.

3 Applicability of technologies for eGovernment users information security protection

There are some basic requirements which must meet in phase of development and implementation of security policies for identified or universal users of eGovernment services [12]:

- minimum need computer skills in eGovermnent users, which mainly will create and implement security policies with their own knowledge. The technologies they will use must be as transparent as is possible;
- minimum need of financial resources for implementing the technologies which will make them available for more citizens who must become eGovernment services users;
- possibilities for easy advance of implemented technologies with users experience and security needs evolution.

Based on information from international Endpoint Protection Platform vendors [4], [5], [7] and from surveys for endpoint security state [3], [6], [11] some conclusions about applicability of anti-theft and data leakage prevention technologies for protection of information security of eGovernment users can be done:

- To be applicable for eGovernment users, Ownership management services must be integrated in the eGovernment services themselves;
- To be more useful for eGovernment users, internal timer protection tool must be implemented as a software module, which is automatically installed when the users register themself for the respective class of eGovernment services. At this moment all protected user sensitive data must be automatically identified and the destructive routine must be transparently configured;
- It would be an advantage if the users can automatically unlock their computer system in case it was found after deactivation and if the user can authenticate himself with eSignature, by example;
- At this moment technologies for sensitive data leakage prevention are too complex for common eGovernment users and can be implemented only with gentle approach for DLP in protection of their information security. Tools who offer customizable set of pre-defined sensitive data type definitions are most suitable and perspective decisions in this direction;
- Some of advantages of DLP technologies can be reached only in integration with automatic and transparent identification of sensitive user data in the process of user registration for eGovernment services and their future protection. Security policy configuration wizards can give the possibilities for selection and customization of embedded sensitive data type definitions to apply, for event and action settings. They can automatically put in protection data such as credit and debit card numbers, bank accounts. national identification numbers, social insurance numbers, fiscal code number, postal adresses, phone numbers, passport details, email adresses, etc;

- Integration of DLP technologies with other services like e-mail, instant messaging, Skype, social networking, etc would be a challenge and a big advantage for eGovernment services users.

References

1. State of Internet security: protecting the network. Webroot software, 2009.
2. L. Zeltser Emerging Internet security threats in 2009.
3. CSI Computer Crime and security survey. CSI, 2009.
4. CISCO Midyear Security Report., CISCO, 2009.
5. Symantec Endpoint Protection - value delivery research study. Symantec Corp., 2009.
6. Magic Quadrant for Endpoint protection platform., Gartner, 2009.
7. Endpoint security and data protection., Sophos, 2009.
8. Filkins, B., D. Radcliff, Data leakage landscape: Where data leaks and how to apply next generation tools., SANS Institute, 2008.
9. Mogull, R. Is DLP keeping your data where it should be?., Information Security magazine, vol.2, 2009.
10. The evolution of endpoint security., Sophos, 2009.
11. State of Endpoint., Ponemon institute, 2009.
12. Palazov, A. Policies and architectures for information security of citizens as users of the eGovernment. Sofia, Alternativi, 2008.